(12)特許協力条約に基づいて公開された国際

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年2 月8 日 (08.02.2001)

PCT

(10) 国際公開番号
WO 01/09735 A1

(51) 国際特許分類[7]: G06F 15/00, H04M 3/42, H04B 7/26

(21) 国際出願番号: PCT/JP00/04399

(22) 国際出願日: 2000 年7 月3 日 (03.07.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/216948 1999 年7 月30 日 (30.07.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 コムスクエア (COMSQUARE CO., LTD.) [JP/JP]; 〒104-0061 東京都中央区銀座三丁目4番12号 文祥堂ビル6F Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 上嶌 靖 (UESHIMA, Yasushi) [JP/JP]; 〒104-0061 東京都中央区銀座三丁目4番12号 文祥堂ビル6F 株式会社コムスクエア内 Tokyo (JP).

(74) 代理人: 後藤洋介, 外 (GOTO, Yosuke et al.); 〒105-0003 東京都港区西新橋1丁目4番10号 第三森ビル Tokyo (JP).

(81) 指定国 (国内): CA, CN, MX, RU, US.

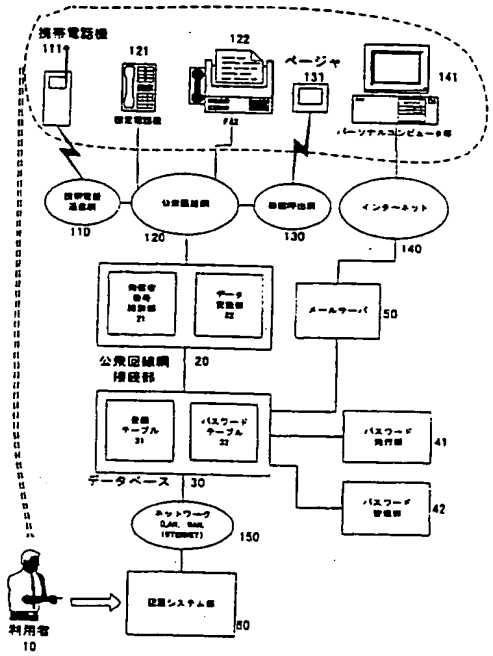
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: AUTHENTICATION METHOD, AUTHENTICATION SYSTEM AND RECORDING MEDIUM

(54) 発明の名称: 利用者認証方法、利用者認証システムおよび記録媒体



(57) Abstract: For the authentication by a service provider, a registered user dials a registered telephone number to connect a CTI (computer telephony integration) server. The CTI server authenticates the user based on the dialed number, generates a password input by the user with the password received from the CTI server, and begins to supply services if the passwords coincide with each other.

[続葉有]

WO 01/09735 A1

(57) 要約:

サービス供給装置が予め登録された利用者を認証する際に、認証に先立って、利用者の電話機の電話番号を登録しておき、この電話機を用いて、利用者が、ＣＴＩ(computer telephony integration)サーバに電話を発呼する。ＣＴＩサーバは着呼した電話番号に基づいて利用者を認証した後、ＣＴＩサーバ等の情報処理装置でパスワードを生成して、利用者およびサービス供給装置の両方に送信する。サービス供給装置は、送信されたパスワードと、利用者が入力したパスワードを比較し、両者が一致する場合、利用者に対してサービスを供給する。

明　細　書

利用者認証方法、利用者認証システムおよび記録媒体

技術分野

本発明は、ＣＴＩ(computer telephony integration)に関し、特に、ＣＴＩ技術を応用したユーザ認証に関する。

背景技術

現代社会において、正規の利用者として予め登録した者（以下、登録者）を認証する技術は社会の様々な局面で用いられている。例えば、通信ネットワークシステム上の情報提供サービスにユーザがアクセスするとき、また、オフィスビルの入口等に設けられる電子錠を解錠するとき等の状況で認証技術が用いられている。

こうした認証技術として古くから用いられているシステムとして、登録者に固定したパスワードを発行し、認証の際にシステムの利用者に対してパスワードの入力を促し、これを登録済みのパスワードと比較して、一致する場合に限り利用者にシステムの利用を認めるものがある。以下、このように原則として固定したパスワードを用いて認証を行う技術を固定パスワード方式と記す。固定パスワード方式は登録者を簡便に認証できる方式だが、登録者には容易に覚えることができると同時に、第三者には想起できないような文字列を生成することは困難であることや、全ての登録者に徹底したパスワード管理を実行させるのは困難であることといった事情があるので、固定パスワード方式は、ハッカーの標的となって繰り返し攻撃を受けると突破される可能性が極めて高い。

固定パスワード方式のこのような欠点を克服するため、従来から様々な技術が提案されている。

一例を挙げると、特開平１０－３３６３４５号公報には、通信ネットワークシステム上の情報提供装置に対して、利用者の情報端末置を接続する際に用いる認証システムが記載されている。このシステムでは、固定パスワード方式に代わり、利用者の情報端末装置の発信者電話番号を利用して登録者を認証するため、パスワードを知得した第三者が、登録された情報端末装置以外の装置を用いて情報提供装置にアクセスするのを防ぐことができる。

しかし、この技術には、例えば、登録者の認証を受ける端末と、情報提供装置のサービスを利用するための端末とが、同一の端末である必要があるといった制約がある。つまり、登録者の情報端末装置が使用する電話番号を登録しているので、未登録の電話番号に接続された情報端末装置を使う場合、登録者といえども認証を受けることはできない。

また、通信ネットワークシステム上の情報提供装置等へのアクセスに関する認証に利用することはできるが、建築物の電子錠を解錠する場合や、銀行のキャッシュディスペンサーにて顧客を認証する場合のように、利用者の端末からアクセスできない情報処理装置等を使用する際の認証には利用できない。

更に、情報端末装置が使用する電話番号を認証するので、同一の情報端末装置を複数の人間が利用する場合に、それぞれの利用者を個別に認証することができない。

このような特開平１０－３３６３４５号公報の技術の他に、固定パスワード方式の問題点の解決しようとする技術として、所謂ワンタイムパスワード方式がある。固定パスワード方式では、システム側または登録者が更新しなければパスワードは不変であるのに対して、ワンタイムパスワード方式では、認証の度毎に新しいパスワードを利用して認証を行う。このため、仮にパスワードが第三者に漏洩しても最小限の被害に食い止めることができる。ワンタイムパスワード方式を採用した従来技術

には、次のようなものがある。

特開平１１－１７８０２２号公報に記載された技術等では、認証サーバと同期して、生成するパスワードを認証の度毎に変更していくパスワード生成器を用いている。認証サーバに認証を要求する際、登録者は、パスワード生成器が生成したパスワードを登録者自身のＩＤと共に認証サーバに送信する。認証サーバはパスワード生成器と同期しているので、認証要求を受けた時点で該ＩＤに対応するパスワードを生成することができる。よって、認証サーバは利用者から受け取ったパスワードと認証サーバ自身が生成したパスワードを比較して利用者を認証することができる。

また、特開平８－２２７３９７号公報や特開平１１－１６１６１８号公報に記載の技術では、予め登録者毎に異なる符号化規則を割り当てて、それぞれの登録者に対し、割り当てられた符号化規則に従って動作する復号化器を持たせる。利用者からＩＤが送信されると、認証サーバは、ランダムにパスワードを生成し、当該ＩＤの利用者に割り当てられた符号化規則に従ってパスワードを符号化後、利用者に送信する。これを受信した利用者は、自分の復号化器を使用してパスワードを復号し、その結果を認証サーバに返信する。認証サーバは、自身が生成したパスワードと、利用者から返信されたデータとを比較して、利用者を認証する。

上述のワンタイムパスワード方式を用いた従来技術では、専用のハードウェア、或いは、専用のソフトウェアとこれを実行可能なハードウェアを、すべての登録者に対して準備する必要がある。こうした専用ハードウェアや専用ソフトウェアはコストが高くなりやすい。また、専用ソフトウェアを実行するために必要なハードウェアとしては、例えば携帯情報機器やノートパソコン等が考えられるが、これらも決して安価なものではなく、普及しつつあるとはいえ誰もが持っているものではないので、やはりコストの問題が生じてしまう。更に、特に専用ハードウェア

の場合、認証を行うためにしか必要のない機器を登録者に持ち歩かせることになり、便宜を損ねてしまう。

本発明が解決しようとする課題は、固定パスワード方式や、特開平１０－３３６３４５号公報に記載の技術のもつ問題点、更に、特開平１１－１７８０２２号公報、特開平８－２２７３９７号公報、特開平１１－１６１６１８号公報等に記載された従来のワンタイムパスワード方式のもつ問題点を解決した、新しいワンタイムパスワード方式の認証技術を提供することである。より具体的に述べると、解決しようとする課題として、本発明は以下に述べる課題を掲げる。

・高価になりやすい認証専用のハードウェア／ソフトウェアが必要ない。

・認証を受ける端末と、サービスを利用するための端末とが、必ずしも同一の端末である必要がない。

・建築物を施錠した電子錠や、現金自動支払機のように、利用者の端末からアクセスできない情報処理装置等の認証にも利用可能である。

・同一の端末を複数の人間が利用する場合でも、利用者を個別に認証することができる。

発明の開示

これらの課題を解決するため、本発明は以下に述べるような利用者認証方法、利用者認証システム、および、利用者認証プログラムを記録した記録媒体を提供する。

（１）利用者認証方法

本発明が提供する利用者認証方法は、サービスを供給する装置（以下、サービス供給装置と記す）が予め登録された利用者を認証する方法において、認証に先立って、利用者の電話機の電話番号を登録する段階(1)と、登録した電話機を用 いて、利用者が、ＣＴＩ(computer telephony integration)サーバに電話を発呼する段階(2)と、ＣＴＩサーバが着呼

した電話番号に基づいて利用者の認証を行 う段階(3)と、ＣＴＩサーバまたはＣＴＩサーバと連係して動作する他の情報処 理装置がパスワードを生成する段階(4)と、生成したパスワードを、利用者およ びサービス供給装置の両方に送信する段階(5)と、受信したパスワードを利用者がサービス供給装置の利用を認証する装置（以下、サービス利用認証装置）に入力する段階(6)と、サービス利用認証装置が、前記段階(5)により受信したパスワードと、前記段階(6)で入力されたパスワードを比較し、両パスワードが一致す る場合、該利用者にサービス供給装置の利用を認める段階(7)と、認証に用いた パスワードを無効にする段階(8)とを含むことを特徴とする利用者認証方法であ る。尚、ここでいうサービス供給装置は例えばＷｅｂサーバ、電子錠、現金自動支払機等の金融自動化機等の利用者に対して直接サービスを供給する装置であり、サービス利用認証装置はこれらのサービスを受けようとする利用者を認証する装置であり、例えば認証サーバ等に相当する。

この利用者認証方法において、パスワード生成後予め定められた時間を経過した場合、利用者がそのパスワードを用いて認証を受けていない場合であっても、そのパスワードを無効にすることとしてもよい。こうすることにより、なんらかの理由で利用者がパスワードを紛失・失念したり、認証を受けずに放置しても、認証の安全性を確保することができる。

段階(1)で電話番号を登録される電話機としては、携帯移動通信端末機が特に 好適である。ここでいう携帯移動通信端末機とは、所謂携帯電話機、ＰＨＳ(personal handy phone system)の端末機のような持ち運び可能な電話機を指す。本 発明では、従来技術のパスワード生成器に近い位置づけの装置として携帯移動通信端末機を用いている。このような携帯移動通信端末機は既に広く普及しているので専用のパスワード生成器を用いる場合と比較してコスト面で有利なばかりではなく、利用者から見

れば認証を受けるためだけに必要なパスワード生成器を所持する必要がないというメリットがある。

段階(5)で利用者に送信されるパスワードの送信先およびそのデータ形式は、利用者が決定することにしてもよい。本発明では、ユーザにパスワードを通知する方法として複数の方法が選択可能であり、この方法は、システムがサポートする通知手段の種類や、利用者の便宜等によって決定されてよい。パスワードの送信には例えば次のようなものがある。

・予め登録された電話番号のページャに対し、文字データとして送信して通知する。

・予め登録された電話番号のファクシミリ装置に対し、画像データとして送信する。

・段階(1)で登録された電話機に対し、音声合成装置にて発せられた音声として 送信する。この場合、段階(3)にて発信者電話番号に基づく認証を受けた後、電 話機とＣＴＩサーバとの間の回線は維持されて音声が電話機に送られる。

・段階(1)で登録された電話機は画像表示手段を備え、段階(5)での利用者へのパスワードの送信は、段階(1)で登録された電話機に対し、文字データとして送信 される。近年の電話機、携帯移動通信端末機の多くが画面表示手段を備えるので、これによれば、パスワードの視覚的な確認を簡便に行うことができる。

・利用者が指定するメールアドレスに電子メールとして送信される。これは、携帯情報端末機やノート型パーソナルコンピュータの普及に鑑みている。尚、インターネット経由の電子メールでは、その内容について完全な守秘性を保つことは難しいが、本発明では、万一パスワードが漏洩したとしてもほとんど問題にならない程度までパスワードの有効期限を短く設定することができるので、システムのセキュリティにほとんど影響がない。

・パスワードをバイナリデータで送信する。この場合、利用者側にもバイナリデータに対応したプログラム等が必要となるが、同時に、何らかの方法でこのバイナリデータを入手した者にとっても、直接にはデータの内容がわからないため、よりシステムの安全性を高めることができる。
・段階(1)で登録された電話機は、無線通信手段を備え、段階(6)でのサービス利用認証装置へのパスワードの入力は、無線通信手段を介して行われる。この場合、利用者がパスワードを手入力する必要がないので、利用者の操作がより簡便になる。また、手入力を介さないため、誤入力の可能性が低くなる。

（２）利用者認証システム

本発明が提供する利用者認証システムは、相互にデータ通信を行って連係して動作する１ないし複数の情報処理装置と、利用者それぞれに割り当てられた電話機とを含んで構成されるシステムであって、電話機と電話回線を介して接続する回線接続手段、回線接続手段に対する着呼の発信者電話番号を識別する発信者番号識別手段、利用者に割り当てられた電話機の電話番号を含む利用者に関する情報を、それぞれの利用者毎に関連付けて、利用者情報として格納する第１の記録媒体、第１の記録媒体を参照し、利用者情報の中の利用者に割り当てられた電話機の電話番号から、発信者番号識別手段が識別した電話番号の有無を検索する電話番号検索手段、パスワードを生成するパスワード生成手段、パスワード生成手段が生成したパスワードを、第１の記録媒体に格納された利用者情報に関連付けて格納する第２の記録媒体、電話番号検索手段で発見された電話番号、または、該電話番号に関連付けられた利用者情報を送信先として参照し、該当する送信先にパスワードを通知するパスワード通知手段、利用者からパスワードの入力を受け付けるパスワード入力手段、第２の記録媒体に格納されたパスワードと、パスワード入力手段から入力されたパスワードを比較し、両パスワードが一致する場合、利用

者を認証する認証手段、および、予め定められた条件を満たすパスワードを、第２の記録媒体から消去または無効にする手段を、情報処理装置のいずれかに備えることを特徴とする利用者認証システムを提供する。

この利用者認証システムでは、利用者それぞれに割り当てられた電話機は、携帯移動通信端末機が特に好適である。

パスワード通知手段は、例えば次のようなものがある。これらの通知手段を複数の種類備えていてもよい。

・パスワード生成手段により生成されたパスワードに相当する音声を合成する音声合成手段を情報処理装置のいずれかに更に備え、パスワード通知手段は、音声合成手段により合成された音声を、電話回線を介して送信する。

・パスワード生成手段により生成されたパスワードに相当するファックス画像データを生成するファックス画像データ生成手段を前記情報処理装置のいずれかに更に備え、パスワード通知手段は、ファックス画像データ生成手段により生成されたファックス画像データを、電話回線を介して送信する。

・パスワード生成手段により生成されたパスワードをページャに表示するデータを生成するページャデータ生成手段を情報処理装置のいずれかに更に備え、パスワード通知手段は、ページャデータ生成手段により生成されたデータを、電話回線を介して送信する。

・パスワード生成手段により生成されたパスワードを記載した電子メールを生成する電子メール生成手段と、インターネットに接続する手段とを情報処理装置のいずれかに更に備え、パスワード通知手段は、電子メール生成手段により生成された電子メールを、インターネットを介して送信する。

パスワードを消去または無効にする条件としては、例えば、パスワード生成手段が該パスワードを生成後に予め定められた時間が経過した場

合、該パスワードによる前回の認証後に予め定められた時間が経過した場合、および、予め定められた回数の認証に該パスワードが利用された場合がある。原則として、パスワードは発行後１回認証に用いると２度と使用できないが、この他にも、利用者の便宜とシステムの安全性とを比較考量して上に述べたような条件でパスワードを消去・無効化してよい。

この利用者認証システムは、人物を認証するシステム全般に適用可能であるが、例えば次のような認証に利用可能である。

・認証手段が、ネットワーク上のコンテンツに対するアクセスを認証する。

・認証手段が、電子錠を制御する装置に接続され、該電子錠の解錠を許可する。

・認証手段が、金融自動化機の利用者の認証を行う。

（３）利用者認証プログラムを記録した記録媒体

本発明が提供する利用者認証プログラムを記録した記録媒体は、１ないし複数の情報処理装置により実行されるプログラムであり、かつ、相互にデータ通信を実行して連係して動作するプログラムを記録した、機械読み取り可能な記録媒体において、利用者に割り当てられた電話機の電話番号を含む利用者に関する情報を、それぞれの利用者毎に関連付けて、利用者情報として格納する第１のテーブルを生成する処理と、電話回線からの着呼の発信者電話番号を識別する発信者番号識別処理と、第１のテーブルを参照し、利用者情報の中の利用者に割り当てられた電話機の電話番号から、発信者番号識別処理により識別された電話番号を検索する電話番号検索処理と、パスワードを生成するパスワード生成処理と、パスワード生成処理が生成したパスワードを、第１のテーブルに格納された利用者情報に関連付けて格納する第２のテーブルを生成する処理と、電話番号検索処理で発見された電話番号、または、該電話番号に

関連付けられた利用者情報を送信先として参照し、該当する送信先にパスワードを通知するパスワード通知処理と、利用者からパスワードの入力を受け付けるパスワード入力処理と、第２のテーブルに格納されたパスワードと、パスワード入力処理で入力されたパスワードを比較し、両パスワードが一致する場合、利用者を認証する認証処理と、予め定められた条件を満たすパスワードを、第２のテーブルから消去する、または、無効にする処理とを情報処理装置に実行させることを特徴とする利用者認証プログラムを格納した記録媒体を提供する。

パスワード通知処理は、例えば次のようなものがある。

・利用者認証プログラムが、パスワード生成処理により生成されたパスワードに相当する音声を合成する音声合成処理を更に含み、パスワード通知処理は、音声合成処理により合成された音声を、電話回線を介して送信する処理を情報処理装置に実行させる。

・利用者認証プログラムは、パスワード生成処理により生成されたパスワードに相当するファックス画像データを生成するファックス画像データ生成処理を更に含み、パスワード通知処理は、ファックス画像データ生成処理により生成されたファックス画像データを、電話回線を介して送信する処理を情報処理装置に実行させる。

・利用者認証プログラムは、パスワード生成処理により生成されたパスワードをページャに表示するデータを生成するページャデータ生成処理を更に含み、パスワード通知処理は、ページャデータ生成処理により生成されたデータを、電話回線を介して送信する処理を情報処理装置に実行させる。

・利用者認証プログラムは、パスワード生成処理により生成されたパスワードを記載した電子メールを生成する電子メール生成処理と、インターネットに接続する処理とを更に含み、パスワード通知処理は、電子メール生成処理により生成された電子メールを、インターネットを介して

送信する処理を情報処理装置に実行させる。

パスワードを消去または無効にする条件としては、例えば、パスワード生成手段が該パスワードを生成後に予め定められた時間が経過した場合、該パスワードによる前回の認証後に予め定められた時間が経過した場合、および、予め定められた回数の認証に該パスワードが利用された場合がある。原則として、パスワードは発行後１回認証に用いると２度と使用できないが、この他にも、利用者の便宜とシステムの安全性とを比較考量して上に述べたような条件でパスワードを消去・無効化してよい。

本記録媒体に記録されたプログラムを利用すれば、人物を認証するシステム全般に適用可能であるが、例えば次のような認証に利用可能である。

・ネットワーク上のコンテンツに対するアクセスを認証する処理を情報処理装置に実行させる。
・電子錠の解錠を許可する処理を情報処理装置に実行させる。
・金融自動化機の利用者の認証を行う処理を情報処理装置に実行させる。

図面の簡単な説明

第１図は、本発明の第１の実施の形態である利用者認証システム１のシステム構成を説明する図である。

第２図は、利用者認証システム１において、利用者がパスワードの発行要求してからパスワードを受信するまでの動作を説明する図である。

第３図は、利用者認証システム１において、利用者がパスワードの発行要求してからパスワードを受信するまでの動作を説明する図である。

第４図は、利用者認証システム１において、利用者がパスワードを受信してから認証システム部６０に認証を受けるまでの動作を説明する図である。

第５図は、利用者認証システム１のパスワード管理フローを説明する図である。

第６図は、本発明の第２の実施の形態であるＡＴＭ利用者認証方法を説明するフローチャートである。

発明を実施するための最良の形態

１．概論

まず、本発明の概略を説明する。本発明では、キャリア業者が提供する発信者ＩＤサービス（発信者電話番号通知サービス）とＣＴＩシステムとを組み合わせて利用者を認証後、パスワードを生成する。生成したパスワードは、利用者の端末機と、利用者が受けようとするサービスを提供する機器を直接に管理している情報処理装置等との両方に送信される。同一のパスワードは原則として只１回あるいは予め定められた規定回数の認証にしか使用できない。また、発行後一定時間を経過したパスワードは未使用であっても無効とするようにしてもよい。

利用者の認証に用いる端末機としては、特に、一般に普及している携帯電話、ＰＨＳ(personal handy phone system)端末等の携帯通信端末機が好適である。認証を受けた利用者は自分の端末機でワンタイムパスワードを受け取る。

利用者は、音声合成装置にて発せられた音声としてパスワードを受け取ってもよい。この場合、利用者端末機には、電話機の基本的な機能だけしか必要ない。また、利用者端末機がディスプレイ装置を備えることを前提とすればテキストデータでもよい。また、発信者ＩＤによる認証と共に、ワンタイムパスワードの送信先を利用者が指定できるようにすれば、ワンタイムパスワードをＦＡＸ、ページャで受信することも可能である。更に、メールアドレスを指定して電子メールとして受信すれば、様々な情報機器で受信可能である。

利用者が実際に利用している機器と、発信者ＩＤに基づいて認証を行う機器は一体である必要はないので、負荷を分散することができる。また、利用者の端末機と認証を行う機器の間は電話回線により接続され、一方、認証を行う機器と利用者が利用しようとする機器との間は何らかの回線で接続される必要があるが、利用者端末と利用目的機器との間は、接続は必須の条件ではなく、全く接続関係がなくてもよい。

更に、赤外線通信手段を備える端末にパスワードを送信し、このデータを赤外線通信手段を利用して利用目的装置に送信して認証すれば、利用者がパスワードを手入力する必要がないので、パスワードの誤った入力を避けることができると共に、利用者の便宜を図ることができる。このとき、パスワードは人間が直接判読できる必要はないのでバイナリデータを用いても構わない。この場合、そのバイナリデータのデータフォーマットに対応したプログラムで赤外線通信を行う必要があるので、万一パスワードを受信されても対応プログラムがなければ不正に認証を受けることができず、更に安全性が高まる。

２．利用者認証システム１の構成

次に、本発明の第１の実施の形態に係る利用者認証システム１について第１図を参照して説明する。

利用者認証システム１では、利用者１０は、携帯電話機１１１を用いてパスワード発行部４１にパスワードの発行・送信を要求する。ここで、携帯電話機１１１は原則として利用者１０だけが使用するものとする。この条件が満足されるのであれば、パスワードの発行を要求する電話機は固定電話機１２１でも構わない。以下では、利用者がパスワードの発行をシステムに要求する際に用いる電話機をパスワード発行要求端末と呼ぶ。パスワード発行要求端末として使用できる端末は、それ自身の電話番号を持つような端末である。このような端末としては、携帯電話機１１１、固定電話機１２１の他に、ＰＨＳ(personal handy phone syst

em)端末、ファクシミリ装置付属の電話機、電話機能を備える携帯情報端末（ＰＤＡ)、モデムやターミナルアダプタが接続されたパーソナルコンピュータ等がある。

一方、利用者１０がパスワードを受け取る場合は、携帯電話機１１１や固定電話機１２１で音声として受け取ってもよいし、携帯電話機１１１や固定電話機１２１に画像表示手段があれば文字として画面表示しても構わない。同様に、ファクシミリ装置１２２、ページャ１３１、パーソナルコンピュータ１４１で受信する事もできる。これら通信端末のように、利用者がシステムからパスワードを受信するために用いる機器を以下では、パスワード受信端末と記す。利用者はパスワード受信端末で受信したパスワードを認証システム部６０に入力し、最終的に認証システム部６０の認証を受ける。

このように、本発明では、利用者が認証を受ける際、パスワード発行要求端末とパスワード受信端末とを用いる事になる。これは、本発明では、発信者電話番号による認証を行う段階と、利用者１０がパスワード発行部４１から受け取ったパスワードと、認証システム部６０がパスワード発行部４１から受け取ったパスワードとを比較して認証を行う段階との２段階の認証を行うためである。尚、後述するようにこれら２種類の端末として同じ端末を兼用する事も可能であるが、この場合、パスワード発行要求端末の機能上の要請により、電話機を用いる事になる。

次に、利用者認証システム１の特徴的な構成要素について説明する。公衆回線網接続部２０は、公衆回線網１２０とデータベース３０とを接続するインタフェースとして働くと共に、利用者の認証（より正確には利用者が認証の際に使用する事になっているパスワード発行要求端末、即ち、携帯電話機１１１、固定電話機１２１の電話番号の認証）に必要な情報を取得する機能を有する。即ち、公衆回線網接続部２０は、着呼の発信者電話番号を識別する発信者番号識別部２１と、パスワード発行

部４１が生成したパスワードを、電話機、ファクシミリ装置、ページャ、電子メール端末等のパスワード受信端末が受信可能なデータ形式に変換するデータ変換部２２とを備える。例えば、パスワード受信端末が電話機である場合、データ変換部２２は音声合成装置を含む。またファクシミリ装置であれば、パスワードの文字列を画像に変換する手段を含む。即ち、利用者認証システム１がパスワード受信端末としてどのような端末をサポートするかにより、データ変換部２２の構成は異なる。

発信者番号識別部２１が識別した発信者電話番号は、データベース３０に送信される。データベース３０は、正規の利用者に関する情報（利用者情報）を格納する登録テーブル３１と、パスワード発行部４１が発行したパスワードを格納するパスワードテーブル３２とを格納している。登録テーブル３１は、利用者が認証を要求する際に使用するパスワード発行要求端末の電話番号を含み、電話番号に関連付けて格納された利用者情報から構成される。他方、パスワードテーブル３２は、特定の利用者１０に対してパスワード発行部４１が発行したパスワードを、登録テーブル３１の該当する利用者に関連付けて格納する。尚、ここでは便宜上２つのテーブルとして説明しているが、ひとつのテーブルでも構わない。また、互いに関連付けられた２つのテーブルとする場合、登録テーブル３１とパスワードテーブル３２とは異なるデータベースで管理されてもよい。発信者番号識別部２１から電話番号を受け取ると、データベース３０は登録テーブル３１を参照し、正規利用者の電話番号として登録されているか否かを検索する。ここで登録テーブル３１に該電話番号が登録されていなければ、データベース３０は公衆回線網接続部２０に回線の切断を指示する。受け取った電話番号が正規利用者のものであれば、データベース３０はパスワード発行部４１にパスワードの生成を指示する。

パスワード発行部４１は、予め設定されたロジックに従ってパスワー

ドを生成する。生成するパスワードは数字、アルファベット、記号、カタカナその他の文字の組み合わせが一般的であるが、他の文字種を使用しても構わない。また、生成するパスワードの文字列の桁数も、固定されていても可変でもどちらでも構わない。

パスワード管理部４２は、パスワードテーブル３２に格納されているパスワードを監視し、所定の条件（パスワード無効化条件）でパスワードを無効にする処理を行う。パスワード無効化条件として、例えば、次のような条件が考えられる。

（条件１）認証システム部６０で該パスワードによる認証をＮ回行った場合。ここでＮは自然数である。このような条件の設定は、例えばパスワードテーブル３２に認証を行った回数を表す項目を追加する事で実現できる。Ｎが小さい方が安全性は高く、最も安全なのはＮ＝１、即ち、同じパスワードでは一度しか認証しないとする条件である。この条件を設定する場合は、認証の回数を記録する代わりに、認証を行ったパスワードをパスワードテーブル３２から削除することにしてもよい。

（条件２）パスワード発行後に一定時間経過後、そのパスワードが認証に使用された回数に関わらず、そのパスワードを無効にする。この条件は、例えば、パスワードテーブル３２にそのパスワードが発行された時刻を記録する項目を設け、一定時間毎にパスワード管理部４２がこの項目をチェックして、予め定められた期間を経過したパスワードを削除することで実現できる。

（条件３）条件１でＮが２以上の時、前回の認証から経過した時間が一定時間を経過するとそのパスワードを無効にする。この条件は、例えば、パスワードテーブル３２にそのパスワードが最後に認証に用いられた時刻を記録する項目を設け、一定時間毎にパスワード管理部４２がこの項目をチェックして、予め定められた期間を経過したパスワードを削除することで実現できる。

（条件４）発行されたパスワードが有効な利用者がパスワードの発行を要求した時、既存のパスワードの利用状況に関わらずパスワードを更新する。

これらの条件は、単独で使用してもよいが、組み合わせて使用した方が有用である。例えば、条件１を採用して同一パスワードによる認証は一度だけとすると共に、条件２を採用し、未認証のパスワードであっても発行後３分を過ぎれば無効になるとすれば、不正に認証を受けようとするのは極めて困難になる。

メールサーバ５０は、データベース３０からパスワードとメールアドレスを受け取り、受け取ったメールアドレスを宛先とし、パスワードを内容とする電子メールを作成して、インターネット１４０を介してメール端末１４１にその電子メールを送信する。メールサーバ５０は、パスワード受信端末であるメール端末１４１に受信可能なデータ形式にパスワードを変換・送信する点で、公衆回線網接続部２０とデータ変換部２２とに相当する機能を持つ事になる。

認証システム部６０は、ネットワーク１５０を介してデータベース３０と接続されており、パスワードテーブル３２のパスワードと利用者１０が入力したパスワードとを用いて利用者１０を認証し、登録された利用者に対して種々のサービスを提供する。ネットワーク１５０はＬＡＮ(local area network)、ＷＡＮ(wide area network)、インターネット等のネットワークである。尚、第１図では、説 明の便宜上、認証システム部６０を１つしか図示していないが、複数の認証システム部６０がネットワーク１５０上に存在してもよく、それぞれの認証システム部６０が異なるサービスを提供しても構わない。サービスの具体例には次のようなものがある。

（例１）ネットワーク上のＷＥＢページの利用者を認証する。この場合、利用者は、認証システム部６０とネットワークを介して接続された

ＷＥＢページを表示可能な端末からそのＷＥＢページにアクセスし、利用者側のパスワード入力をこのＷＥＢ端末から行うことになる。

（例２）建築物のドアに設けられた電子錠を解錠する利用者を認証する。この場合、電子錠は、パスワードの入力を受け付ける入力装置を備える必要がある。例２では、利用者１０がパスワード発行要求端末およびパスワード受信端末を兼ねる端末として、赤外線通信装置等の無線通信手段を備える携帯電話機を用いる実施の形態がある。即ち、パスワードの発行要求と発行されたパスワードの受信を同一の携帯電話機により行って、受信したパスワードを無線通信手段で送信する。これに対し、電子錠側も無線通信手段を備えて、携帯電話機から無線通信を経由してパスワードを受け付けるようにする。このような実施の形態では、利用者自らがパスワードを入力するのに比べ、入力の手間が省略できる、誤入力の恐れが低い等の利用者の便宜が図ることができる。

（例３）銀行等のＡＴＭ(automated teller machine)で本人を認証する。現在一般に普及しているＡＴＭでは、磁気カードと固定の暗証番号との組み合わせにより本人を認証しているが、これに代わり、磁気カードと本発明で利用者が受け取るパスワードとの組み合わせにより本人を認証する。この場合、パスワードを第三者が推測する事は極めて困難なので、磁気カードを紛失したり盗難されたりしても悪用される恐れが低い。尚、パスワード発行要求端末の利用者を、パスワード発行要求端末にて認証する機構を具備するのが望ましい。このようなパスワード発行端末としては、例えば、予めパスワードを入力しない限り、一切の操作ができないような携帯電話機がある。

３．利用者認証システム１の動作

次に、利用者認証システム１で、利用者１０がパスワードの発行を要求してから認証システム部６０でサービスを受けるまでの過程を説明する。

（１）パスワード発行要求からパスワード発行まで

利用者がパスワードの発行を要求してからパスワードが発行されるまでの過程の概略は次の通りである。

①利用者情報の登録：登録テーブル３１に利用者情報を登録する。

②パスワード発行の要求：利用者がパスワード発行要求端末を使ってパスワードの発行を要求する。

③パスワードの生成：パスワードを生成する。

④パスワードの通知：パスワードをパスワード受信端末に送信する。

⑤パスワードによる認証：利用者が入力するパスワードと生成されたパスワードとを比較して利用者を認証する。

⑥パスワードの無効化：パスワード無効化条件を満たすパスワードを無効にする。

以下にこの過程をより詳しく説明する。

①利用者情報の登録

利用者認証システム１により認証を受けようとする者は、次のような情報（利用者情報）をデータベース３０に登録しておく必要がある。

（ａ）パスワード要求端末の電話番号。必須の情報である。同一の利用者が複数の電話番号を登録してもよい。

（ｂ）ユーザ名。利用者認証システム１における利用者の識別子としての名前である。認証システム部６０が利用者を認証する際にユーザ名とパスワードの組を用いる場合に必要になる。認証をパスワードのみで行う場合は不要である。

（ｃ）ファクシミリ装置の電話番号。該利用者がパスワードを受信するために利用する端末（以下、パスワード受信端末と記す）が、ファクシミリ装置であれば必要になる。

（ｄ）ページャの電話番号。利用者のパスワード受信端末がページャである場合必要になる。

（ｅ）電子メールのアドレス。該利用者がパスワードを電子メールとして受信する場合に必要となる。

（ｆ）パスワード無効化条件。利用者毎にパスワード無効化条件を設定する場合に必要。

（ｇ）その他のユーザ情報。氏名、年齢、生年月日、住所等。サービスの必要等に応じて登録する。

②パスワード発行の要求

③パスワードの生成

④パスワードの通知

次に利用者がパスワードの発行を要求してからパスワードを受け取るまでの利用者認証システム１の動作を説明する。ところで、②のパスワード発行の要求において、利用者認証システム１は、発信者電話番号通知サービスを利用して電話をかけてきた利用者の認証を行うが、このとき、必ずしも呼が接続されなくてもよい。即ち、発信者電話番号を通知する信号は、回線の確立に先立って送信される信号なので、公衆回線網接続部２０は呼を接続する事なく利用者を認証する事ができる。そこで、ここでは（ａ）公衆回線網接続部２０が着呼を接続する場合、および、（ｂ）公衆回線網接続部２０が着呼を接続しない場合、の２つの動作を説明する。

（ａ）公衆回線網接続部２０が着呼を接続する場合の動作

第２図を参照して説明すると、まず、利用者はパスワード発行要求端末を用いて公衆回線網接続部２０に電話をかける（ステップＳ１）。すると、電話通信事業者は、パスワード発行要求端末のＩＤ（電話番号）を公衆回線網接続部２０に通知する。発呼元が発信者電話番号を非通知に設定していて発信者番号が通知されない場合や、認識した電話番号が登録テーブル３１に登録されていない場合、公衆回線網接続部２０は着信を拒否するか、または自動着信してエラーメッセージを送信後に回線を

切断する（ステップＳ３）。

発信者番号を通知する設定がされており、通知された番号が登録テーブル３１に登録されたものであれば、公衆回線網接続部２０は自動着信する（ステップＳ５）。

パスワード発行に、利用者のユーザー名が必要な場合には、利用者認証システム１は、ユーザー名の入力を音声にて利用者に要求する（ステップＳ７）。この要求に応じて、利用者はパスワード発行要求端末からユーザ名を入力する（ステップＳ８）。入力の手段としては、パスワードが数字のみから構成されるのであれば、パスワード発行要求端末の数字キーを用いて入力する。パスワードが数字以外の文字・記号等を含む場合も同様に数字キーから入力してもよい。この場合、文字や記号にそれぞれ固有のコードが割り当てて、利用者は数字キーからコードを入力して文字等を入力する。また、文字・記号等の入力を簡単にするために、公衆回線網接続部２０に音声認識装置を設け、利用者がパスワードを発声して入力する事にしてもよい。

データベース２０は、入力されたユーザ名が通知された発信者電話番号のユーザ名として登録されているものと一致しているか否かを、登録テーブル３１を参照して判定し（ステップＳ９）、一致していない場合は利用者にユーザ名の再入力を促して判定を繰り返す（ステップＳ９）。数回繰り返してもユーザ名が正しく入力されない場合、パスワード発行要求端末にエラーメッセージを表示して接続を断つ（ステップＳ１０）。

ユーザ名が登録テーブル３１に登録されているものと一致する場合、もしくは、パスワード発行要求にあたってユーザ名の入力を利用者に求めない場合、データベース３０はパスワード発行部４１にパスワードの発行を要求する（ステップＳ１１）。これを受けたパスワード発行部４１は、予め設定された一定のロジックに基づいてパスワードを生成する（ステップＳ１２）。パスワードはパスワードテーブル３２に登録される（ス

テップＳ１３）と共に利用者のパスワード受信端末に送信される（ステップＳ１４）。例えば、パスワード発行要求端末とパスワード受信端末とをファクシミリ装置で兼ねる場合、利用者はファクシミリ装置に付属の受話器を用いて認証を受けた後も回線を維持し、そのまま続けてデータ変換部２２がファクシミリ画像データに変換したパスワードを受信すればよい。また、パスワード受信端末としてページャを用いる場合、データ変換部２２でページャで表示可能なデータ形式に変換後、利用者のページャに送信すればよい。更に、パスワード受信端末としてメール受信端末を利用する場合、メールサーバ５０がパスワードを記載した電子メールを利用者のメールアドレス宛に送信する。

（ｂ）公衆回線網接続部２０が着呼を接続しない場合の動作

続いて、パスワード発行要求を行う際に、パスワード発行要求端末と公衆回線網接続部２０との間に回線を確立しない場合の利用者認証システム１の動作を、第３図を参照して説明する。

利用者は、パスワード発行要求端末を用い、電話通信事業者の回線網を介して、公衆回線網接続部２０に電話をかけ、呼出音を数回鳴動させた後、電話を切る（ステップＴ１）。この際、公衆回線網接続部２０は発信者電話番号を示す信号は受信するが、呼の接続は行わない。この呼が発信者電話番号を非通知に設定された電話機からなされている場合、その呼は無視される（ステップＴ３）。

発信者番号識別部２１が発信者の電話番号を識別した場合、その電話番号はデータベース３０に渡される。データベース３０は、登録テーブル３１に登録された全利用者のパスワード発行要求端末の電話番号から、その電話番号の登録の有無を検索する（ステップＴ２）。ここで該当する電話番号が登録テーブル３１に存在しない場合、そのパスワード発行要求は無視される（ステップＴ３）。

該当する電話番号が登録されている場合、データベース３０は、パス

ワード発行部４１にパスワードの発行を要請する（ステップＴ５）。これを受けたパスワード発行部４１は、一定のロジックに従ってパスワードを発行する（ステップＴ５）。

発行されたパスワードは、パスワードテーブル３２に登録される（ステップＴ７）と共に、公衆回線接続部２０またはメールサーバ５０から利用者のパスワード受信端末に送信される（ステップＴ８）。具体的には既に述べたステップＳ１４に関する説明と同じであるので省略する。

⑤パスワードによる認証

上述のようにパスワードを受け取った利用者は、そのパスワードを認証システム部６０に入力して認証システム部６０の認証を受ける。次に、第４図を参照して、発行されたパスワードを用いて認証システム部６０が利用者を認証する時の動作を説明する。

認証システム部６０は、利用者からパスワードのみ、あるいはユーザ名とパスワードの組の入力を受け付ける。この際、ここで利用者が使用する入力装置は、パスワードを利用者から受け取るため認証システム部６０に設けられたキーボード等の入力装置である。入力装置として他に、赤外線通信装置等の無線通信手段がある。即ち、認証システム部６０とパスワード受信端末との両方にデータ通信可能な無線通信手段を設け、上述の②～④の過程でパスワード受信端末が受信したパスワードを、無線通信を利用して認証システム部６０に送信するものである。

認証にユーザ名が必要な場合、利用者は、認証システム部６０の入力装置からユーザ名を入力する（ステップＵ２、Ｕ３、Ｕ４）。このときにユーザ名が登録されていなければ、認証システム部６０はその利用者の認証をしない（ステップＵ９）。

ユーザ名が登録されている場合、または、認証にユーザ名を使用しない場合、利用者が認証システム部６０にパスワードを入力すると、認証システム部６０はパスワードを受け付けて（ステップＵ５、Ｕ６、Ｕ７）

パスワードのマッチングを行う（ユーザ名を用いる場合はユーザ名とパスワードの組み合わせに対してマッチングを行う)。ここでマッチすれば認証システム部６０はその利用者を認証し（ステップＵ８)、しなければ認証を拒否する（ステップＵ９)。

発行されたパスワードは、パスワード発行プログラムにより、データベースシステム上に登録される。ユーザー名がある場合には、パスワードをユーザー名と関連付けて登録する。

書き込まれたパスワードは、一定時間データベースシステム上に保存されるが、設定された条件になった場合には、パスワード管理プログラムによって、消去あるいは無効となる。

ユーザ名が必要な場合、パスワード発行プログラムは、発行されたパスワードをユーザ名と関連付けてデータベースシステムに登録する。

⑥パスワードの無効化

第５図のように、所定の条件を満たすパスワードは、パスワード管理プログラムにより削除または無効化される（ステップＶ１)。

ここで、所定の条件には例えば次のようなものがある。

・利用者がそのパスワードを使って認証を受けた回数を条件とする場合。このとき、１回でも認証を受けたパスワードは無効にしてもよいし、認証に利用可能な回数を設定しておいてもよい。

・パスワード発行後の経過時間を条件とする場合。例えば、パスワード発行後６０分を経過したものは、たとえ認証を受けていなくとも、無効にする。

・そのパスワードで前回認証を受けた時から経過した時間を条件とする場合。

４．第２の実施の形態

次に、第２の実施の形態として、携帯電話機を用いてＡＴＭ(automated teller machine)の利用者認証を行う実施の形態を説明する。ここで

ＡＴＭは認証システム部６０に相当する。また、ここで用いる携帯電話機は、電子メール受信端末としての機能と、赤外線通信等の無線通信インタフェースを備えるものとする。また、ＡＴＭも携帯電話機に対応する無線通信インタフェースを備えるものとする。

利用者は、自分の携帯電話機から公衆回線網接続部２０に電話をかけて、パスワードの発行依頼をする（ステップＷ１）。

データベース３０は発信者番号識別部２１が識別した発信者の電話番号を登録テーブル３１内に検索し、マッチすれば正規の利用者として認証する。これに対して、パスワード発行部４１がパスワードを発行し、発行されたパスワードはパスワードテーブル３２に格納されると共にメールサーバ５０を介し、電子メール受信端末としての携帯電話機に送信される（ステップＷ２）。この際、パスワードをテキストデータとしてではなくバイナリーデータの暗号として送信し、このバイナリデータに対応するデコードプログラムで処理した後、パスワードとして利用できるようにして、正規の利用者の携帯電話機でこのデコードプログラムが実行できるようにしておけば、万一パスワードデータを含む電子メールを第三者が傍受したとしても、このデコードプログラムがない限り、認証に使用すべきパスワードは入手できない事になり、より一層システムの安全度を高める事ができる。

こうしてパスワードを受け取った後、利用者は、ＡＴＭの動作モードを変更し、パスワードを受信可能な動作状態に変更する（ステップＷ３）。そして、無線通信インタフェースを介して、携帯電話機からＡＴＭにパスワードを送信する（ステップＷ４）。尚、この無線通信インタフェースによるパスワード送信機能を利用する際には、携帯電話機が利用者にパスワードの入力を求めるようにして、携帯電話の紛失・盗難等に起因するリスクを抑える事が望ましい。

携帯電話機からパスワードを受信すると、ＡＴＭはデータベース３０

にアクセスして、受信したパスワードが認証を受けたものであるか否かを問い合わせる。パスワードテーブル３２にパスワードが登録されていれば、利用者は正規の者として認証されて、ＡＴＭによる銀行口座の操作が認められるようになる（ステップＷ６）。パスワードテーブル３２に該当するパスワードが登録されていなければ、その利用者による銀行口座の操作は拒絶される（ステップＷ７）。

尚、ここで挙げた利用者識別システムの構成は例であり、本発明のシステムを構成する各要素は、ネットワーク上に分散して配置された複数の情報処理装置によって実行される分散処理であっても実現可能である事は、当業者には明らかである。

例えば、利用者認証システム１ではデータベース３０に登録テーブル３１とパスワードテーブル３２とが両方格納されているが、パスワードテーブル３２は認証システム部６０に格納されていても、同様の効果が得られるのは明らかである。

産業上の利用可能性

本発明によれば、現在既に広く普及している電話機を利用して利用者の認証を行うので、認証専用のハードウェアが必要な従来の技術に比べて低いコストで同等の効果を得る事ができる。特に、携帯電話機や簡易型携帯電話機を用いると便利である。

また、本発明では、パスワード発行要求端末とパスワード受信端末とが必ずしも同じである必要がないので、利用者の置かれた状況に応じて最も都合のいい形でパスワードを受信する事ができる。

また、建築物を施錠した電子錠や、現金自動支払機のように、利用者の端末からアクセスできない情報処理装置等の認証にも利用可能である。

更にまた、同一の端末を複数の人間が利用する場合でも、認証の際にユーザ名を併用することにより、利用者を個別に認証することができる。

以上、本発明を実施の形態に基づいて説明したが、本発明はこれに限定されるものではなく、当業者の通常の知識の範囲内でその変更や改良が可能であることは勿論である。

請求の範囲

1．サービスを供給する装置（以下、サービス供給装置と記す）が予め登録された利用者を認証する方法において、

認証に先立って、利用者の電話機の電話番号を登録する段階(1)と、

登録した電話機を用いて、利用者が、ＣＴＩ(computer telephony integration)サーバに電話を発呼する段階(2)と、

ＣＴＩサーバが着呼した電話番号に基づいて利用者の認証を行う段階(3)と、

ＣＴＩサーバまたはＣＴＩサーバと連携して動作する他の情報処理装置がパスワードを生成する段階(4)と、

生成したパスワードを、利用者およびサービス供給装置の両方に送信する段階(5)と、

受信したパスワードを利用者がサービス供給装置の利用を認証する装置（以下、サービス利用認証装置）に入力する段階(6)と、

サービス利用認証装置が、前記段階(5)により受信したパスワードと、前記段 階(6)で入力されたパスワードを比較し、両パスワードが一致する場合、該利用 者にサービス供給装置の利用を認める段階(7)と、

認証に用いたパスワードを無効にする段階(8)と

を含むことを特徴とする利用者認証方法。

2．請求項1に記載の利用者認証方法において、パスワード生成後予め定められた時間を経過した場合、利用者がそのパスワードを用いて認証を受けていない場合であっても、そのパスワードを無効にすることを特徴とする利用者認証方法。

3．請求項1に記載の利用者認証方法において、前記段階(1)で電話番号を登録される電話機は、携帯移動通信端末機である ことを特徴とする利用者認証方法。

4．請求項1に記載の利用者認証方法において、前記段階(5)で利用者に送信されるパスワードの送信先およびそのデータ形 式は、利用者が決定することを特徴とする利用者認証方法。

5．請求項1に記載の利用者認証方法において、前記段階(5)での利用者へのパスワードの送信は、予め登録された電話番号 のページャに対し、文字データとして送信されることを特徴とする利用者認証方法。

6．請求項1に記載の利用者認証方法において、前記段階(5)での利用者へのパスワードの送信は、予め登録された電話番号 のファクシミリ装置に対し、画像データとして送信されることを特徴とする利用者認証方法。

7．請求項1に記載の利用者認証方法において、前記段階(5)での利用者へのパスワードの送信は、前記段階(1)で登録された電話機に対し、音声合成装置にて発せられた音声として送信されることを特徴とする利用者認証方法。

8．請求項1に記載の利用者認証方法において、前記段階(1)で登録された電話機は画像表示手段を備え、前記段階(5)での利用者へのパスワードの送信は、前記段階(1)で登録された電話機に対し、文字デ ータとして送信されることを特徴とする利用者認証方法。

9．請求項1に記載の利用者認証方法において、前記段階(5)での利用者へのパスワードの送信は、利用者が指定するメール アドレスに電子メールとして送信されることを特徴とする利用者認証方法。

10．請求項1に記載の利用者認証方法において、前記段階(5)にて利用者に送信されるパスワードは、バイナリデータであ ることを特徴とする利用者認証方法。

11．請求項1に記載の利用者認証方法において、前記段階(1)で登録された電話機は、無線通信手段を備え、前記段階(6)でのサービス利用認証装置へのパスワードの入力は、無線通信手段を介して行われることを特徴とする利用者認証方法。

１２．相互にデータ通信を行って連係して動作する１ないし複数の情報処理装置と、利用者それぞれに割り当てられた電話機とを含んで構成されるシステムであって、

電話機と電話回線を介して接続する回線接続手段と、

前記回線接続手段に対する着呼の発信者電話番号を識別する発信者番号識別手段と、

利用者に割り当てられた電話機の電話番号を含む利用者に関する情報を、それぞれの利用者毎に関連付けて、利用者情報として格納する第１の記録媒体と、

前記第１の記録媒体を参照し、前記利用者情報の中の利用者に割り当てられた電話機の電話番号から、前記発信者番号識別手段が識別した電話番号の有無を検索する電話番号検索手段と、

パスワードを生成するパスワード生成手段と、

前記パスワード生成手段が生成したパスワードを、前記第１の記録媒体に格納された利用者情報に関連付けて格納する第２の記録媒体と、

前記電話番号検索手段で発見された電話番号、または、該電話番号に関連付けられた利用者情報を送信先として参照し、該当する送信先にパスワードを通知するパスワード通知手段と、

利用者からパスワードの入力を受け付けるパスワード入力手段と、

前記第２の記録媒体に格納されたパスワードと、前記パスワード入力手段から入力されたパスワードを比較し、両パスワードが一致する場合、利用者を認証する認証手段と、

予め定められた条件を満たすパスワードを、前記第２の記録媒体から消去または無効にする手段と

を、前記情報処理装置のいずれかに備えることを特徴とする利用者認証システム。

１３．請求項１２に記載の利用者認証システムにおいて、前記利用者そ

れぞれに割り当てられた電話機は、携帯移動通信端末機であることを特徴とする利用者認証システム。

１４．請求項１２に記載の利用者認証システムにおいて、

前記パスワード生成手段により生成されたパスワードに相当する音声を合成する音声合成手段を前記情報処理装置のいずれかに更に備え、

前記パスワード通知手段は、前記音声合成手段により合成された音声を、電話回線を介して送信する

ことを特徴とする利用者認証システム。

１５．請求項１２に記載の利用者認証システムにおいて、

前記パスワード生成手段により生成されたパスワードに相当するファックス画像データを生成するファックス画像データ生成手段を前記情報処理装置のいずれかに更に備え、

前記パスワード通知手段は、前記ファックス画像データ生成手段により生成されたファックス画像データを、電話回線を介して送信する

ことを特徴とする利用者認証システム。

１６．請求項１２に記載の利用者認証システムにおいて、

前記パスワード生成手段により生成されたパスワードをページャに表示するデータを生成するページャデータ生成手段を前記情報処理装置のいずれかに更に備え、

前記パスワード通知手段は、前記ページャデータ生成手段により生成されたデータを、電話回線を介して送信する

ことを特徴とする利用者認証システム。

１７．請求項１２に記載の利用者認証システムにおいて、

前記パスワード生成手段により生成されたパスワードを記載した電子メールを生成する電子メール生成手段と、インターネットに接続する手段とを前記情報処理装置のいずれかに更に備え、

前記パスワード通知手段は、前記電子メール生成手段により生成され

た電子メールを、インターネットを介して送信する
ことを特徴とする利用者認証システム。

１８．請求項１２に記載の利用者認証システムにおいて、前記予め定められた条件は、

前記パスワード生成手段が該パスワードを生成後に予め定められた時間が経過した場合、

該パスワードによる前回の認証後に予め定められた時間が経過した場合、および、

予め定められた回数の認証に該パスワードが利用された場合
のいずれかであることを特徴とする利用者認証システム。

１９．請求項１２に記載の利用者認証システムにおいて、前記認証手段は、ネットワーク上のコンテンツに対するアクセスを認証することを特徴とする利用者認証システム。

２０．請求項１２に記載の利用者認証システムにおいて、前記認証手段は、電子錠を制御する装置に接続され、該電子錠の解錠を許可することを特徴とする利用者認証システム。

２１．請求項１２に記載の利用者認証システムにおいて、前記認証手段は、金融自動化機の利用者の認証を行うことを特徴とする利用者認証システム。

２２．１ないし複数の情報処理装置により実行されるプログラムであり、かつ、相互にデータ通信を実行して連係して動作するプログラムを格納した、機械読み取り可能な記録媒体において、

利用者に割り当てられた電話機の電話番号を含む利用者に関する情報を、それぞれの利用者毎に関連付けて、利用者情報として格納する第１のテーブルを生成する処理と、

電話回線からの着呼の発信者電話番号を識別する発信者番号識別処理と、

前記第１のテーブルを参照し、前記利用者情報の中の利用者に割り当てられた電話機の電話番号から、前記発信者番号識別処理により識別された電話番号を検索する電話番号検索処理と、

パスワードを生成するパスワード生成処理と、

前記パスワード生成処理が生成したパスワードを、前記第１のテーブルに格納された利用者情報に関連付けて格納する第２のテーブルを生成する処理と、

前記電話番号検索処理で発見された電話番号、または、該電話番号に関連付けられた利用者情報を送信先として参照し、該当する送信先にパスワードを通知するパスワード通知処理と、

利用者からパスワードの入力を受け付けるパスワード入力処理と、

前記第２のテーブルに格納されたパスワードと、前記パスワード入力処理で入力されたパスワードを比較し、両パスワードが一致する場合、利用者を認証する認証処理と、

予め定められた条件を満たすパスワードを、前記第２のテーブルから消去する、または、無効にする処理と

を情報処理装置に実行させることを特徴とするプログラムを格納した記録媒体。

２３．請求項２２に記載の記録媒体において、

前記プログラムは、前記パスワード生成処理により生成されたパスワードに相当する音声を合成する音声合成処理を更に含み、

前記パスワード通知処理は、前記音声合成処理により合成された音声を、電話回線を介して送信する処理を情報処理装置に実行させる

ことを特徴とする記録媒体。

２４．請求項２２に記載の記録媒体において、

前記プログラムは、前記パスワード生成処理により生成されたパスワードに相当するファックス画像データを生成するファックス画像データ

生成処理を更に含み、

前記パスワード通知処理は、前記ファックス画像データ生成処理により生成されたファックス画像データを、電話回線を介して送信する処理を情報処理装置に実行させる

ことを特徴とする記録媒体。

２５．請求項２２に記載の記録媒体において、

前記プログラムは、前記パスワード生成処理により生成されたパスワードをページャに表示するデータを生成するページャデータ生成処理を更に含み、

前記パスワード通知処理は、前記ページャデータ生成処理により生成されたデータを、電話回線を介して送信する処理を情報処理装置に実行させる

ことを特徴とする記録媒体。

２６．請求項２２に記載の記録媒体において、

前記プログラムは、前記パスワード生成処理により生成されたパスワードを記載した電子メールを生成する電子メール生成処理と、インターネットに接続する処理とを更に含み、

前記パスワード通知処理は、前記電子メール生成処理により生成された電子メールを、インターネットを介して送信する処理を情報処理装置に実行させる

ことを特徴とする記録媒体。

２７．請求項２２に記載の記録媒体において、前記予め定められた条件は、

前記パスワード生成処理が該パスワードを生成後に予め定められた時間が経過した場合、

該パスワードによる前回の認証後に予め定められた時間が経過した場合、および、

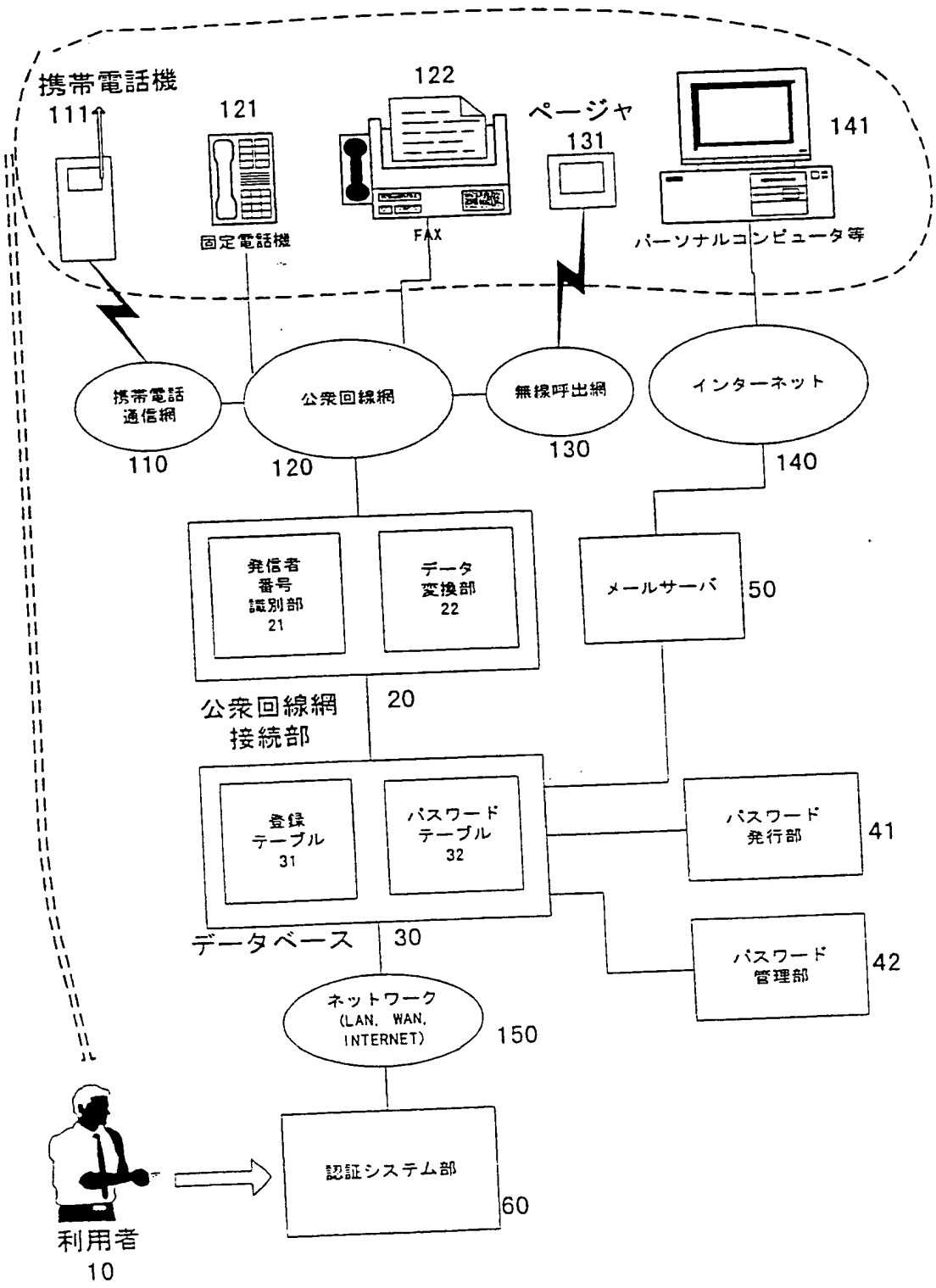
予め定められた回数の認証に該パスワードが利用された場合
のいずれかであることを特徴とする記録媒体。

２８．請求項２２に記載の記録媒体において、前記認証処理は、ネットワーク上のコンテンツに対するアクセスを認証する処理を情報処理装置に実行させることを特徴とする記録媒体。

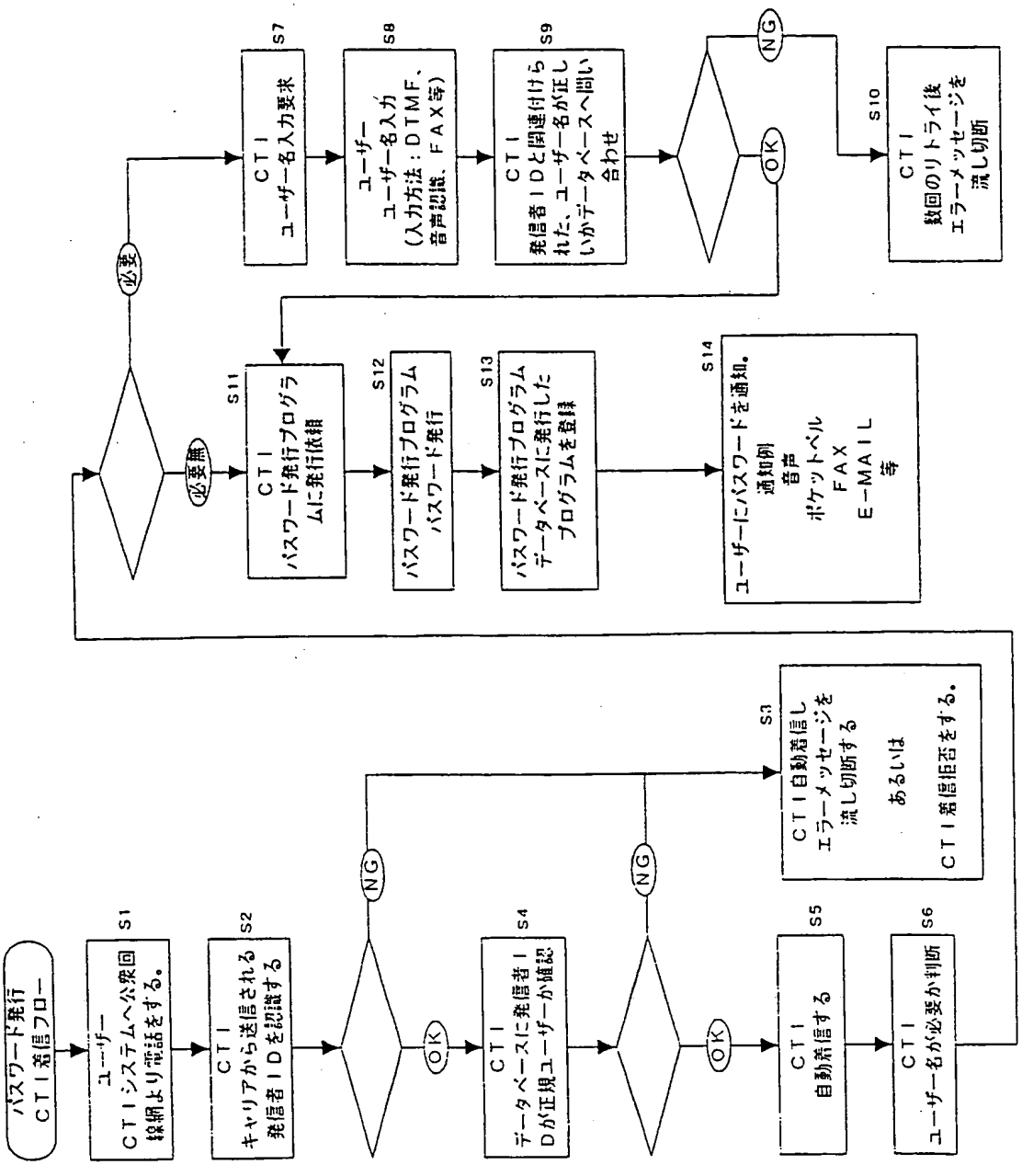
２９．請求項２２に記載の記録媒体において、前記認証処理は、電子錠の解錠を許可する処理を情報処理装置に実行させることを特徴とする記録媒体。

３０．請求項２２に記載の記録媒体において、前記認証処理は、金融自動化機の利用者の認証を行う処理を情報処理装置に実行させることを特徴とする記録媒体。

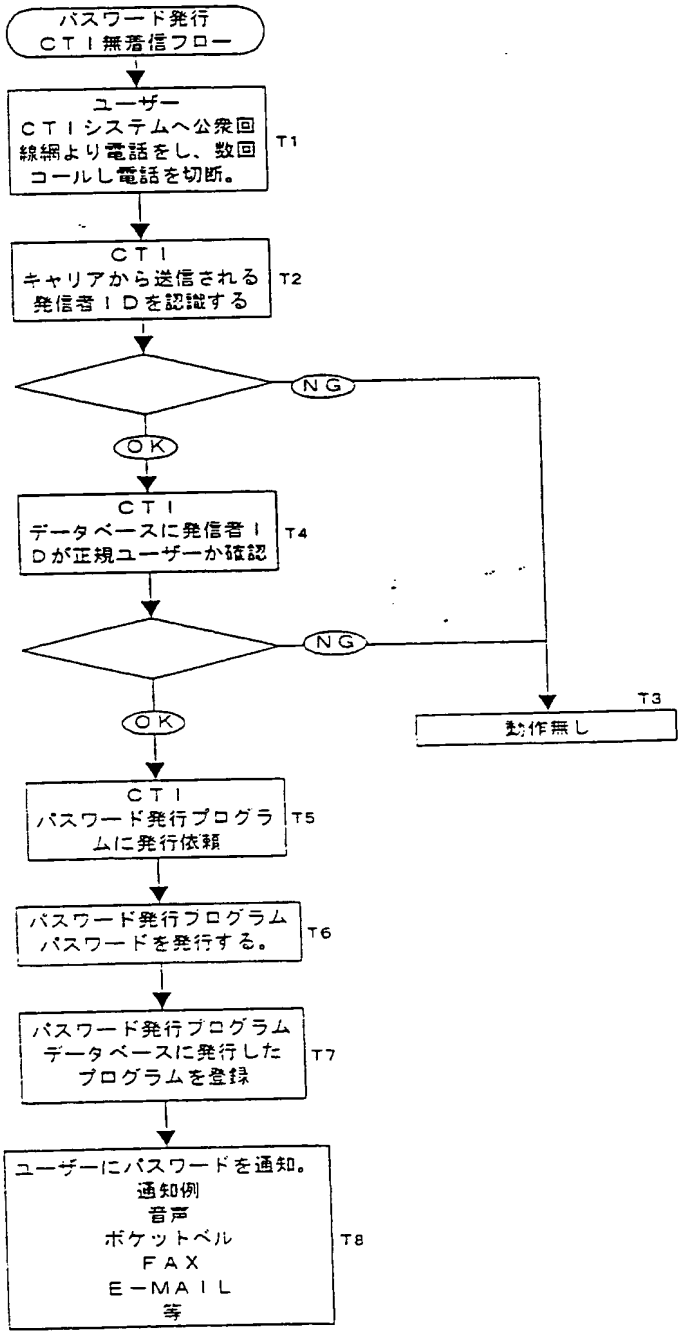
第 1 図


携帯電話機
111
121
固定電話機
122
FAX
ページャ
131
141
パーソナルコンピュータ等
携帯電話
通信網
110
公衆回線網
120
無線呼出網
130
インターネット
140
発信者
番号
識別部
21
データ
変換部
22
メールサーバ
50
公衆回線網
接続部
20
登録
テーブル
31
パスワード
テーブル
32
パスワード
発行部
41
データベース
30
パスワード
管理部
42
ネットワーク
(LAN、WAN、
INTERNET)
150
認証システム部
60
利用者
10

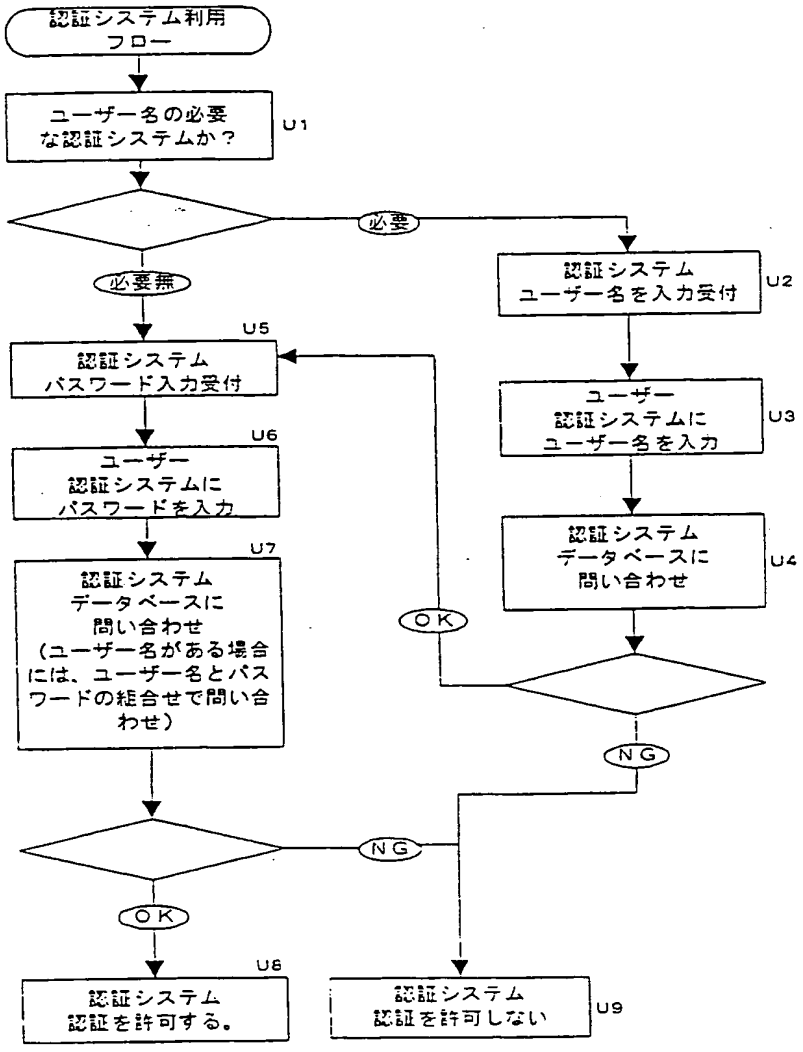
第 2 図


パスワード発行
CTI着信フロー
ユーザー
CTIシステムへ公衆回線網より電話をする。
S1
CTI
キャリアから送信される発信者IDを認識する
S2
NG
OK
CTI
データベースに発信者IDが正規ユーザーか確認
S4
NG
OK
CTI
自動着信する
S5
CTI
ユーザー名が必要か判断
S6
必要
必要無
CTI
ユーザー名入力要求
S7
ユーザー
ユーザー名入力
(入力方法：DTMF、音声認識、FAX等)
S8
CTI
発信者IDと関連付けられた、ユーザー名が正しいかデータベースへ問い合わせ
S9
NG
OK
CTI
数回のリトライ後エラーメッセージを流し切断
S10
CTI
パスワード発行プログラムに発行依頼
S11
パスワード発行プログラム
パスワード発行
S12
パスワード発行プログラム
データベースに発行したプログラムを登録
S13
ユーザーにパスワードを通知。
通知例
音声
ポケットベル
FAX
E-MAIL
等
S14
CTI自動着信し
エラーメッセージを流し切断する
あるいは
CTI着信拒否をする。
S3

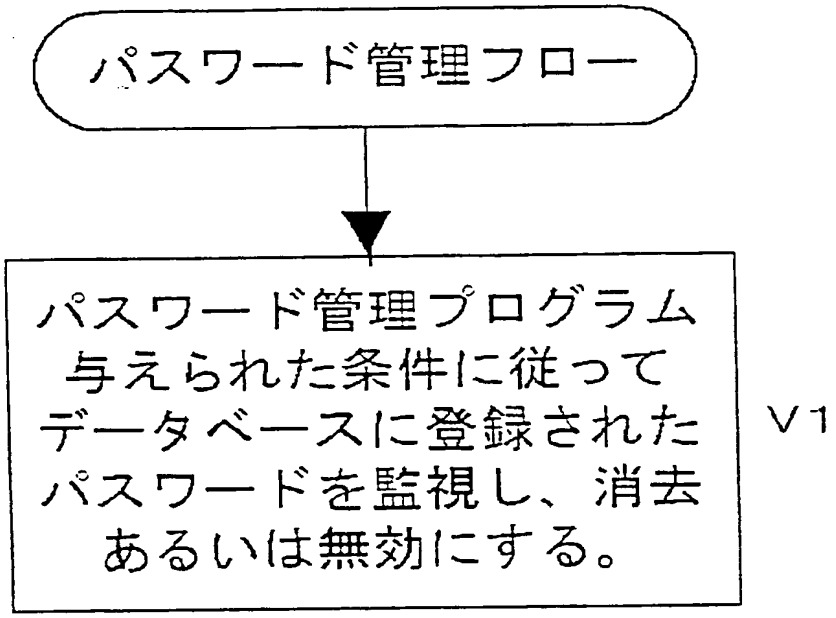
第 3 図


パスワード発行
ＣＴＩ無着信フロー
ユーザー
ＣＴＩシステムへ公衆回線網より電話をし、数回コールし電話を切断。
T1
ＣＴＩ
キャリアから送信される発信者ＩＤを認識する
T2
NG
OK
ＣＴＩ
データベースに発信者ＩＤが正規ユーザーか確認
T4
NG
OK
T3
動作無し
ＣＴＩ
パスワード発行プログラムに発行依頼
T5
パスワード発行プログラム
パスワードを発行する。
T6
パスワード発行プログラム
データベースに発行したプログラムを登録
T7
ユーザーにパスワードを通知。
通知例
音声
ポケットベル
ＦＡＸ
Ｅ－ＭＡＩＬ
等
T8

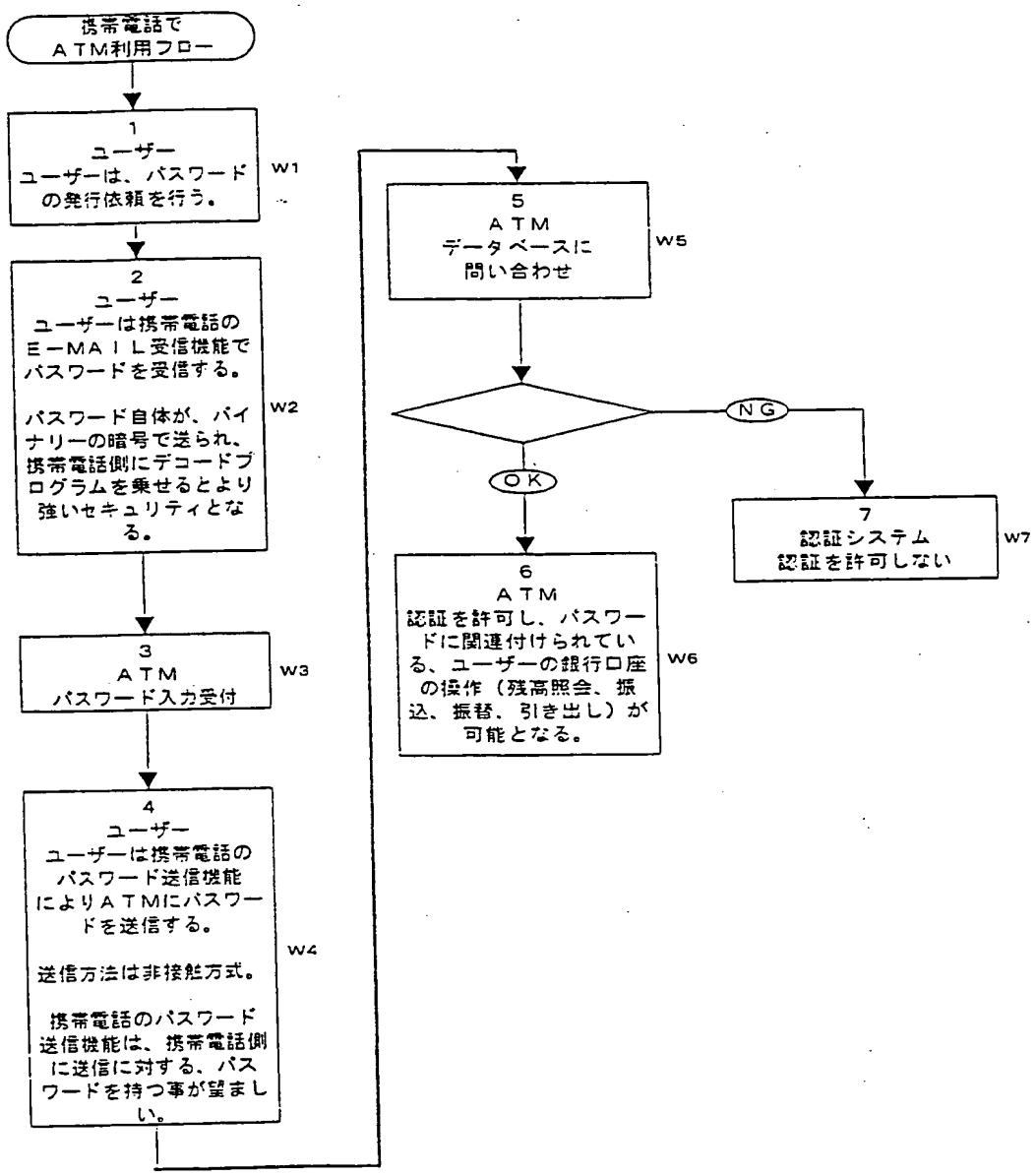
第 4 図


認証システム利用フロー
ユーザー名の必要な認証システムか？
U1
必要
必要無
認証システムユーザー名を入力受付
U2
ユーザー認証システムにユーザー名を入力
U3
認証システムデータベースに問い合わせ
U4
OK
NG
U5
認証システムパスワード入力受付
U6
ユーザー認証システムにパスワードを入力
U7
認証システムデータベースに問い合わせ（ユーザー名がある場合には、ユーザー名とパスワードの組合せで問い合わせ）
NG
OK
U8
認証システム認証を許可する。
認証システム認証を許可しない
U9

第　5　図


パスワード管理フロー
パスワード管理プログラム
与えられた条件に従って
データベースに登録された
パスワードを監視し、消去
あるいは無効にする。
V1

第 6 図


携帯電話で
ＡＴＭ利用フロー
1
ユーザー
ユーザーは、パスワードの発行依頼を行う。
W1
2
ユーザー
ユーザーは携帯電話のＥ－ＭＡＩＬ受信機能でパスワードを受信する。
パスワード自体が、バイナリーの暗号で送られ、携帯電話側にデコードプログラムを乗せるとより強いセキュリティとなる。
W2
3
ＡＴＭ
パスワード入力受付
W3
4
ユーザー
ユーザーは携帯電話のパスワード送信機能によりＡＴＭにパスワードを送信する。
送信方法は非接触方式。
携帯電話のパスワード送信機能は、携帯電話側に送信に対する、パスワードを持つ事が望ましい。
W4
5
ＡＴＭ
データベースに問い合わせ
W5
NG
OK
6
ＡＴＭ
認証を許可し、パスワードに関連付けられている、ユーザーの銀行口座の操作（残高照会、振込、振替、引き出し）が可能となる。
W6
7
認証システム
認証を許可しない
W7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04399

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, H04M 3/42, H04B 7/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, H04M 3/42, H04B 7/26, H04L 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST Science Technology Document Database,
mobile, cellular, authentication, one-time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP, 861461, A2 (Schmitz, Kim), 16 January, 1998 (16.01.98), See the full text & DE, 19718103, A1 & AU, 9863545, A & JP, 10-341224, A & CN, 1207533, A & US, 6078908, A	1-10,12-30 11
X Y	JP, 11-120397, A (NTT POWER AND BUILOING FACILITIES INC.), 30 April, 1999 (30.04.99), See the full text (Family: none)	1-4,7,8,10, 12-14,20,22, 23,29 11
EX	JP, 2000-10927, A (NEC Yonezawa Ltd.), 14 January, 2000 (14.01.00), See the full text (Family: none)	1-4,8-10,12,13 ,17,19,22,26,2 8
Y	EP, 686905, A (SUN MICROSYSTEMS, INC.), 13 December, 1995 (13.12.95), Column 8, lines 30 to 33 & JP, 8-227397, A & US, 5604803, A & US, 5732137, A	2,18,27

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 October, 2000 (10.10.00)	24 October, 2000 (24.10.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04399

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-229459, A (Nippon Telegr. & Teleph. Corp. <NTT>), 25 August, 1998 (25.08.98), Column 8, lines 18 to 41 (Family: none)	7,14,19,23,28

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０４３９９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl' G06F15/00, H04M 3/42, H04B 7/26

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl' G06F15/00, H04M 3/42, H04B 7/26, H04L 9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２６－１９９６年
日本国公開実用新案公報	１９７１－２０００年
日本国実用新案登録公報	１９９６－２０００年
日本国登録実用新案公報	１９９４－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＷＰＩ，ＪＩＣＳＴ科学技術文献データベース　mobile, cellular, authentication, one-time

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	EP, 861461, A2(Schmitz, Kim)16.1月.1998(16.01.98),全文を参照 & DE, 19718103, A1 & AU, 9863545, A & JP, 10-341224, A &	1-10, 12-30
Y	CN, 1207533, A & US, 6078908 ,A	11
X	JP, 11-120397, A(株式会社エヌ・ティ・ティ・ファシリティーズ) 30.4月.1999(30.04.99), 全文を参照, ファミリなし	1-4, 7, 8, 10, 12-14. 20, 22, 23, 29
Y		11

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日　１０．１０．００	国際調査報告の発送日　24.10.00
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｍ　９３６４ 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５９９

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０４３９９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
ＥＸ	JP, 2000-10927, A(米沢日本電気株式会社)14.1月.2000(14.01.00) 全文を参照，ファミリなし	1-4, 8-10, 12, 13, 17, 19, 22, 26, 28
Ｙ	EP, 686905, A(SUN MICROSYSTEMS, INC.) 13.12月.1995(13.12.95) 第8欄第30-33行 & JP, 8-227397, A & US, 5604803, A & US, 5732137, A	2, 18, 27
Ｙ	JP, 10-229459, A(日本電信電話株式会社)25.8月.1998(25.08.98) 第8欄第18-41行，ファミリなし	7, 14, 19, 23, 28